BURSOR & FISHER, P.A.
L. Timothy Fisher (State Bar No. 191626)
Joel D. Smith (State Bar No. 244902)
Frederick J. Klorczyk III (State Bar. No. 320783)
Neal J. Deckant (State Bar No. 322946)
1990 North California Boulevard, Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-Mail: ltfisher@bursor.com
jsmith@bursor.com
fklorczyk@bursor.com
ndeckant@bursor.com

BURSOR & FISHER, P.A.
Scott A. Bursor (State Bar No. 276006)
888 Seventh Avenue
New York, NY 10019
Telephone: (212) 989-9113
Facsimile: (212) 989-9163
E-Mail: scott@bursor.com

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

JEREMIAH REVITCH, individually and on behalf of all others similarly situated,

Plaintiff,

v.

NEW MOOSEJAW, LLC and NAVISTONE, INC.,

Defendants.

Case No. 3:18-cv-06827-VC

PLAINTIFF'S COMBINED OPPOSITION TO DEFENDANT MOOSEJAW'S AND NAVISTONE'S SEPARATE MOTIONS TO DISMISS PLAINTIFF'S FIRST AMENDED CLASS ACTION COMPLAINT

Date: May 2, 2019
Time: 10:00 a.m.
Judge: Judge Vince Chhabria

TABLE OF CONTENTS

TABLE OF AUTHORITIES

PAGE(S)

CASES

STATUTES

RULES

I. INTRODUCTION

Defendants have "secretly embedded" wiretaps "in the computer code" on Defendant New Moosejaw, LLC's ("Moosejaw") website, which are then "used by Defendants to scan the user's computer in search of files that can be used to de-anonymize and identify the user, and also to observe visitors' keystrokes, mouse clicks and other electronic communications in real time for the purpose of gathering Personally Identifiable Information ('PII') to de-anonymize those visitors – that is, to match previously unidentifiable website visitors to obtain their names and home addresses, along with detailed data concerning their browsing habits." *Id.* ¶ 1. These wiretaps "enable Defendants to immediately, automatically, and secretly observe the keystrokes, mouse clicks, and other electronic communications of visitors regardless of whether the visitor ultimately makes a purchase" from Moosejaw. *Id.*

In *Cohen v. Casper Sleep Inc.*, 2018 WL 3392877, at *9 (S.D.N.Y. July 12, 2018), the district court found that substantially similar allegations were "unsettling," "disturbing," and "troubling," but nonetheless concluded that it was required to dismiss the claims because federal and New York state law did not provide a remedy. But that is not the case here. Unlike in *Cohen*, Plaintiff Jeremiah Revitch brings claims pursuant to the California Constitution, California statutes, and California common law, none of which were at issue in the *Cohen* matter, and all of which *do* provide a remedy.

II. ARGUMENT

A. Plaintiff States Common Law Claims For Intrusion Upon Seclusion And Invasion Of Privacy

1. Defendants' Arguments For Dismissal Fail Under *Opperman*

"A privacy violation based on the common law tort of intrusion has two elements." *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 285 97 (2009). "First, the defendant must intentionally intrude into a place, conversation, or matter as to which the plaintiff has a reasonable expectation of privacy." *Id.* This means "the defendant must have 'penetrated some zone of physical or sensory privacy … or obtained unwanted access to data' by electronic or other covert means, in violation of the law or social norms." *Shulman v. Group W Prods., Inc.*, 18 Cal. 4th 200, 231 (1998)). Second,

"the intrusion must occur in a manner highly offensive to a reasonable person." *Id.* "California tort law provides no bright line on ['offensiveness']; each case must be taken on its facts." *Hernandez*, 47 Cal. 4th at 287 (quoting *Shulman,* 18 Cal. 4th at 237). Collection of intimate or sensitive personally identifiable information may amount to a highly offensive intrusion. *See*, *e.g.*, *Goodman v. HTC Am., Inc.*, 2012 WL 2412070, at *14-15 (W.D. Wash. June 26, 2012); *In re Vizio, Inc. Consumer Privacy Litig.*, 238 F. Supp. 3d 1204, 1233 (C.D. Cal. 2017) (same). In addition, "substantial privacy interests are at stake when digital data is involved." *Riley v. California*, 573 U.S. 373, 375 (2014).

Judge Tigar's decision in *Opperman v. Path, Inc.*, 87 F. Supp. 3d 1018 (N.D. Cal. 2014) is instructive. There, the plaintiffs alleged that certain software programs offered by Apple surreptitiously "accessed and uploaded information from customers' iDevices without their knowledge, including contact information." *Id.* at 1032. In analyzing whether the elements of an intrusion upon seclusion claim were adequately alleged, the *Opperman* court focused on the fact that cell phones and similar devices contain a wealth of information, and the programs copied plaintiff's address books without "consent or any prompt." *See id.* at 1059.

As for the "highly offensive" element, the *Opperman* court explained that courts should "'consider the degree of intrusion, the context, conduct and circumstances surrounding the intrusion as well as the intruder's motives and objectives, the setting into which he intrudes, and the expectations of those whose privacy is invaded.'" *Id.* at 1060 (quoting *Miller v. Nat'l Broad. Co.*, 187 Cal. App. 3d 1463, 1483-84 (Cal. App. 1986). The court rejected the argument that secretly acquiring personal information is "routine commercial behavior," and concluded that whether the conduct at issue was "highly offensive" was a factual dispute "best left for a jury." *Id.* at 1061; *see also Opperman v. Path*, 205 F. Supp. 3d 1064, 1079 (N.D. Cal. 2016) ("[I]t is possible that a jury … might conclude, as Yelp suggests, that Yelp's conduct was 'far from highly offensive' … [but] a jury might also find the intrusion highly offensive based on both the degree of intrusion (uploading the email addresses of a user's contacts to the Defendants' servers) and the setting in which the invasion took place (users' personal cellular phones)").

Like the defendants in *Opperman*, Defendants here mischaracterize this case as being about run-of-the-mill internet transactions and "routine commercial behavior." Hence, Defendant Moosejaw argues it would be "patently unreasonable" for Plaintiff to expect "communications" with Moosejaw on its website to be private. Moosejaw MTD at 12. But the premise of Defendants' argument is wrong. This is not a case where the plaintiff complains that the defendant uses information obtained after an Internet customer provides information and then hits a "submit" button or finalizes a sale. Instead, Defendant NaviStone, Inc.'s ("NaviStone") code secretly "scans the visitor's computer" and spies in real time on "keystrokes, mouse clicks and other electronic communications … as soon as the visitor loads Moosejaw.com onto their web browser." FAC ¶¶ 13, 33. This interception and scanning occurs "regardless of whether the user completes the form or clicks 'Submit.'" *Id.* ¶ 13 (emphasis added). If Moosejaw's salespeople obtained information by secretly rummaging through the wallets and purses of customers browsing in Moosejaw's brick-and-mortar stores, Defendants' argument that their conduct involves mere "communications" with its customers would be a nonstarter. But that is analogous to what Defendants are doing to Moosejaw's Internet customers.

Defendants also cannot legitimately claim that NaviStone's code is unoffensive, "routine commercial behavior," given that NaviStone uses "dummy domains" to "conceal its activities" from consumers. *Id.* ¶ 17. There would be no reason to employ "dummy domains" if reasonable consumers would not find such monitoring to be offensive. Nor can Defendants downplay the importance of the information obtained from consumers, given that NaviStone boasts about the "wealth of new marketing data" secretly obtained from them. *Id.* ¶ 11. The Gizmodo and Consumerist articles referenced in the FAC further support an inference that reasonable people would be surprised and offended by software that surreptitiously gathers information as soon as a customer visits a website. *See id.* ¶¶ 18, 21. Privacy policies posted on Moosejaw's website count for nothing because "by the time a user reaches the privacy policy, the wiretaps have already been deployed, and the de-anonymization has already occurred." *Id.* ¶ 23.

When presented with the same allegations and the same defendant, the court in *Cohen v. Casper Sleep Inc.*, 2018 WL 3392877, at *4, 9 (S.D.N.Y. July 12, 2018) reluctantly dismissed

federal wiretap claims after noting the allegations were "unsettling," "disturbing," and "troubling." Unlike in *Cohen*, however, California common law provides a remedy where federal law does not. In short, there is no basis to hold as a matter of law that the conduct alleged here fails to state a claim for intrusion upon seclusion and invasion of privacy. As in *Opperman*, the question of whether the conduct alleged is "highly offensive" is a question "best left for a jury." *Opperman*, 87 F. Supp. 3d at 1061.

2. Defendants' Authorities Do Not Support The Proposition That Secret, Nonconsensual Monitoring Is "Routine Commercial Behavior"

Defendants' arguments for dismissal on the pleadings rest on an extreme position with potentially far-reaching implications: they are asking the Court to hold, as a matter of law, that the "routine monitoring of web activity for marketing purposes" is unoffensive and can never support a claim for intrusion upon seclusion or invasion of privacy. Moosejaw MTD at 13; NaviStone MTD at 14. Defendants primarily rely on *Folgestrom*, *In re iPhone Application Litigation*, and *Low*, but none of them support the position advanced by Defendants here.[1] The *Opperman* court addressed the first two of these decisions, and declined to give them such an expansive interpretation.

"In *Folgestrom*, the plaintiff alleged that the defendant retailer routinely asked for customers' zip codes, asked a credit agency to match their zip codes and credit card numbers to home mailing addresses, and then engaged in mail marketing using the addresses. The court first concluded that the plaintiffs did not have a legally protected private interest in their mailing addresses. The court also held that the retailer's conduct was not egregious, but routine commercial behavior." *Opperman*, 87 F. Supp. 3d at 1060-61 (explaining *Folgestrom*) (internal quotations omitted). The court in *Opperman* concluded that *Folgestrom* was "distinguishable" in part because *Folgestrom* did not involve the "surreptitious theft of personal" information. *Id.* Contrary to the positions advanced by Defendants here, the *Opperman* court declined to hold as a matter of law that the surreptitious acquisition of information qualified as unoffensive, "routine commercial behavior." *Id.*

[1] *Folgestrom v. Lamps Plus, Inc.*, 195 Cal. App. 4th 986 (Cal. App. 2011), *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040 (N.D. Cal. June 12, 2012) ("*In re iPhone*"), and *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1025 (N.D. Cal. 2012).

The *Opperman* court also declined to follow *In re iPhone Application Litigation*, explaining it was "not persuaded by cases that have mechanically applied *Folgelstrom* to invasion of privacy claims." *Opperman*, 205 F. Supp. 3d at 1078 (citing, e.g., *In re iPhone Application Litigation*). As the *Opperman* court explained:

> [*In re iPhone Application Litigation*] involved the disclosure to third parties of an iDevice user's unique device identifier number, personal data, and geolocation information. … That court held without explanation that "[e]ven assuming this information was transmitted without Plaintiffs' knowledge and consent, a fact disputed by Defendants, such disclosure does not constitute an egregious breach of social norms," citing *Folgelstrom*. *Id.* As noted above, however, *Folgelstrom* addressed different facts than those in *iPhone Application Litigation*, and the latter court did not explain how expansion of *Folgelstrom's* holding, counter to the privacy interests of iDevice users, was consistent with California's community privacy norms.

Id. at 1078-79 (emphasis added).[2]

Finally, NaviStone argues that "[t]his case is on all fours with *Low*," but that is wrong. *Low* involved tracking cookies, which have become routine, and the cookies disclosed only LinkedIn users' browsing history without disclosing their names or other personal information. *See Low*, 900 F. Supp. 2d at 1016, 1025. Unlike here, the *Low* court emphasized that there was no allegation that the defendant "de-anonymized" the data to reveal the identities of users. *Id.* at 1025. At least one other district court has distinguished *Low* and held that "more routine data collection practices may be highly offensive if a defendant disregards consumers' privacy choices" when collecting data. *In re Vizio, Inc. Consumer Privacy Litig.*, 238 F. Supp. 3d 1204, 1233 (C.D. Cal. 2017) (distinguishing *Low* and holding allegation that Vizio collected data without disclosure supported invasion of privacy claim) (internal quotations omitted). That reasoning is based on the common-sense principle that "users are entitled to deny consent." *Id.*

Here, unlike in *Low*, one of the primary purposes of NaviStone's software is to obtain a "wealth of new marketing data" and to de-anonymize that data even if customers choose not to

[2] *Opperman*'s critique of cases that extended *Folgelstrom* too far also applies to two other decisions cited by Defendant Moosejaw that followed *Folgelstrom*: *Yunker v. Pandora Media, Inc.*, 2013 WL 1282980, at *14-15 (N.D. Cal. Mar. 26, 2013), and *In re Google Android Consumer Privacy Litig.*, 2013 WL 1283236, at *2 (N.D. Cal. Mar. 26, 2013).

disclose his or her identity. FAC ¶¶ 11; *see also e.g.*, *id.* ¶ 16 (alleging that NaviStone's code de-anonymizes the PII of visitors to Moosejaw's website); ¶ 19 (NaviStone boasts that its technology allows it to identify "previously unidentifiable website visitors"); ¶ 20 (quoting from NaviStone's explanation of how the code works); ¶ 21 ("before you hit 'submit,' this company has already logged your personal data"). In short, none of the authorities cited by Defendants support dismissal.

3. Moosejaw's Footnoted Argument Concerning The Right To Privacy Claim Lacks Merit

Defendants' arguments for dismissal of the intrusion upon seclusion claim and the right to privacy claim are mostly based on the same arguments and authorities. In a footnote, however, Moosejaw argues that the right to privacy claim fails for the additional reason that no "legally protected" privacy right is implicated here. Moosejaw MTD at 12. As a preliminary matter, the argument is procedurally improper. "A footnote is the wrong place for substantive arguments on the merits of a motion, particularly where such arguments provide independent bases for dismissing a claim not otherwise addressed in the motion." *First Advantage Background Servs. Corp. v. Private Eyes, Inc.*, 569 F. Supp. 2d 929, 935 n.1 (N.D. Cal. Mar. 5, 2008).

The substance of the argument also fails. The California Supreme Court recognizes two general types of privacy interests that can support a right to privacy claim: "(1) interests in precluding the dissemination or misuse of sensitive and confidential information ('informational privacy'); and (2) interests in making intimate personal decisions or conducting personal activities without observation, intrusion, or interference ('autonomy privacy')." *Hill v. Nat'l Collegiate Athletic Assn.*, 865 P.2d 633, 654 (Cal. 1994). The scanning and surreptitious monitoring of personal computers for personal profit falls well-within the ambit of the first prong. *See Riley*, 573 U.S. at 375 (digital data involves "substantial privacy interests"); *In re Vizio*, 238 F. Supp. 3d at 1231 (denying motion to dismiss right to privacy claim where the defendant tracked video viewing history). Likewise, as for the second prong, online shoppers have a right to know if their "personal activities" and information are being observed without regard for whether they complete a transaction or hit "submit" on a button requesting such information.

The only authority Moosejaw offers in support of its footnoted argument is *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016 (N.D. Cal. 2014). In that case, "Yahoo's Additional Terms of Service expressly informed users that, 'by scanning and analyzing such communications content, Yahoo collects and stores the data.' … Yahoo's consent page also told users that Yahoo would scan their e-mails for a variety of purposes, including to provide 'targeted advertising.' No equivalently explicit consent is present here."[3] *Opperman*, 87 F. Supp. 3d at 992 (explaining and distinguishing *In re Yahoo*); *see also In re Vizio*, 238 F. Supp. 3d at 1232 (same).

B. Plaintiff States Claims Under CIPA

1. Plaintiff States A Claim Under Section 631

Section 631 prohibits wiretapping or "any other unauthorized connection" with a "wire, line, cable, or instrument." *In re Google Inc.*, 2013 WL 5423918, at *15 (N.D. Cal. Sept. 26, 2013) (citing Cal. Penal Code § 631(a)). NaviStone argues that "[t]here is no plausible inference of unlawful interception by NaviStone" because "*Moosejaw* is alleged to have intercepted … communications to which it was a party, conduct not actionable under sections 631." NaviStone MTD at 11 (emphasis added). That is meritless. Even if a Section 631 cannot stand against Moosejaw since it was a party to the alleged communications (which it can), that does not mean that NaviStone is somehow off the hook. *In re Google Inc.*, 2013 WL 5423918, at *15 (N.D. Cal. Sept. 26, 2013) (quoting *Tavernetti v. Superior Court*, 583 P.2d 737, 741 (Cal. 1978)) ("The California Supreme Court has held that section 631 protects against three distinct types of harms: 'intentional wiretapping, [or] willfully attempting to learn the contents or meaning of a communication in transit over a wire, … [or] attempting to use or communicate information obtained as a result of engaging in either of the previous two activities.'").

Similarly, Moosejaw insists that because it "is a party to the purportedly intercepted 'communications' [it] … cannot be held liable under Section 631." Moosejaw MTD at 4. This is nothing but a consent defense. "Under CIPA, a consent defense is established when both parties –

[3] As noted above, any purported privacy policy is irrelevant because "[b]y the time a user reaches the privacy policy, the wiretaps have already deployed, and the de-anonymization has already occurred." FAC ¶ 23.

the sender and the recipient of the communication – consent to the alleged interception." *Matera v. Google Inc.*, 2016 WL 5339806, at *7 (N.D. Cal. Sept. 23, 2016) (citing Cal. Penal Code § 631(a)) (emphasis added). That defense fails here. Plaintiff alleges that he "and Class Members did not consent to any of Defendants' actions in implementing NaviStone's wiretaps on Moosejaw.com. Nor have Plaintiff or Class Members consented to Defendants' intentional access, interception, reading, learning, and collection of Plaintiff and Class Members' electronic communications." FAC ¶ 60; *see also Campbell v. Facebook Inc.*, 77 F. Supp. 3d 836, 848 (N.D. Cal. 2014) ("[A]ny consent with respect to the processing and sending of messages itself does not necessarily constitute consent to the specific practice alleged in this case – that is, the scanning of message content for use [to de-anonymize Plaintiff and Class members]. … Facebook argues that plaintiffs' claim under section 631 fails … [because] plaintiffs consented to any alleged interception. This argument is identical to the 'consent' argument addressed above, and the court rejects it for the same reasons.").

As for Moosejaw, regardless of its status as a purported party to the communication, it nonetheless is liable under Section 631 for its role in helping NaviStone implement its code. As Judge Whyte explained in denying a motion to dismiss a Section 631 claim:

> As plaintiffs point out, however, CIPA provides for recovery against anyone "who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things" prohibited by the statute. Cal. Penal Code § 631; *see also* Cal. Penal Code § 637.2 ("[a]ny person who has been injured by a violation of this chapter may bring an action against the person who committed the violation").

In re: Lenovo Adware Litig., 2016 WL 6277245, at *8 (N.D. Cal. Oct. 27, 2016) (emphasis added). Here, as in *Lenovo*, Plaintiff alleges that Moosejaw "aided, agreed with, or conspired with" NaviStone to violate the CIPA. *See*, *e.g.*, FAC ¶ 44 ("Defendants' actions are and have been intentional as evidenced by, *inter alia*, their design and implementation of the software wiretaps on Moosejaw.com, their use of wiretaps to access files on visitors' computers that are unrelated to the Moosejaw.com website, and their disclosures and uses of the intercepted data files and communications for profit."); FAC ¶ 45 ("Defendants' actions are not part of routine Internet functionality. Wiretaps are not necessary or needed to operate an e-commerce website. The NaviStone code is novel.").

Defendants also argue that "Plaintiff fails to allege that the contents of a communication were obtained, in part because he never explains what, if any, content Moosejaw intercepted." Moosejaw MTD at 5; NaviStone MTD at 11 ("Here, however, no such interception of 'contents' or 'meaning' of any communications is plausibly alleged."). But Plaintiff is not required to plead such details. *See, e.g.*, *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 139 (3d Cir. 2015) ("Because the complaint pleads a broad scheme in which the defendants generally acquired and tracked the plaintiffs' internet usage, we are satisfied that this scheme, if it operated as alleged, involved the collection of at least some 'content' within the meaning of the Wiretap Act."); *Rackemann v. LISNR, Inc.*, 2017 WL 4340349, at *5 (S.D. Ind. Sept. 29, 2017) (denying motion to dismiss interception claim, stating that plaintiff is not required to plead the details of the intercepted communications because "this is not a fraud case" subject to heightened pleading requirements). In any case, Plaintiff's allegations sufficiently set forth what was intercepted. *See* FAC ¶ 5 ("Mr. Revitch's keystrokes, mouse clicks, and other electronic communications were intercepted in real time and were disclosed to NaviStone through Moosejaw's use of NaviStone's wiretap. In doing so, Defendants gathered Mr. Revitch's PII, including his keystrokes, mouse clicks, and other electronic communications. Defendants also scanned Mr. Revitch's computer in search of files that could be used to deanonymize him. As a result of these activities, Defendants then de-anonymized and identified Mr. Revitch as a visitor to Moosejaw.com.").

Defendants further complain that this data "is not an 'electronic communication' within the meaning of Section 631." Moosejaw MTD at 5. As NaviStone explains, "[b]rowsing data – as opposed to actual form field information – is not 'content' of a communication within the meaning of CIPA." NaviStone MTD at 11.[4] That is incorrect. It has been well-established by several circuit courts that "content" under both CIPA and the federal Wiretap Act is broadly defined:

[4] NaviStone points to the declaration of Thomas White, ECF No. 31-1, to argue that "the FAC itself quotes code showing that none of the 'content' or 'meaning' of any communications was transmitted by Moosejaw to NaviStone." NaviStone MTD at 11. The Court should refuse to consider this declaration because "the contents of a declaration or a deposition are not clearly established 'facts' and therefore are inappropriate for judicial notice." *Oracle Am., Inc. v. Hewlett Packard Enter. Co.*, 2017 WL 635291, at *2 (N.D. Cal. Feb. 16, 2017) (quoting *Burnell v. Marin Humane Soc'y*, 2015 WL 6746818, at *2 n.1)). *See also Levitt v. Yelp! Inc.*, 2011 WL 5079526, at *3 (N.D. Cal. Oct. 26, 2011) ("The Court also notes that Plaintiffs have not been afforded an opportunity to conduct discovery. Thus, permitting a Rule 12(b)(1) challenge based on facts asserted by Yelp would be

> The ECPA also says that "'contents,' when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8). This definition encompasses personally identifiable information such as a party's name, date of birth, and medical condition. *See Gelbard* [*v. U.S.*], 408 U.S. [41,] 51 n. 10, 92 S.Ct. 2357. *See generally Nix v. O'Malley*, 160 F.3d 343, 346 n.3 (6th Cir.1998) ("federal wiretap statute[] broadly define[s] 'contents'").

In re Pharmatrak, Inc., 329 F.3d at 18 (emphasis added). Additionally, in *In re Google Inc.*, the Third Circuit explained that even URL addresses qualify as "content" under the Wiretap Act:

> [P]ost-domain name portions of the URL are designed to communicate to the visited website which webpage content to send the user … between the information revealed by highly detailed URLs and their functional parallels to post-cut-through digits, we are persuaded that – at a minimum – some queried URLs qualify as content.

In re Google Inc., 806 F.3d at 139; *In re U.S. for an Order Authorizing the Use of a Pen Register & Trap*, 396 F. Supp. 2d 45, 50 (D. Mass. 2005) ("contents" include URL "subject lines, application commands, search queries, requested file names, and file paths"). *In re Zynga Privacy Litigation*, 750 F.3d 1098, 1109 (9th Cir. 2014), does not compel the opposite conclusion. While the Ninth Circuit held that certain "header information" may not qualify as "content," it also held that URLs are "content" where – as here – they include "search term[s] or similar communication[s] made by the user[.]" *Id.*; *see also* FAC ¶ 34 (screenshot of a user browsing a shopping page for "Moosejaw Men's The Jack Pullover Hoody," at https://www.moosejaw.com/product/moosejaw-men-s-the-jack-pullover-hoody_10273018).

Finally, NaviStone argues that "Plaintiff does not plausibly allege that NaviStone read any communications 'in transit.'" NaviStone MTD at 11 (emphasis added). That is not required. *See Moreno v. Valenzuela*, 2017 WL 1534276, at *8 (E.D. Cal. Apr. 28, 2017) ("Here it was defendant who transmitted the pictures taken by the cameras that he secretly installed. But the statute, quoted ante, does not require that the victim actually transmit, only that the defendant intercept the

---

inappropriate."); *Patel v. Facebook Inc.*, 290 F. Supp. 3d 948 (N.D. Cal. 2018) ("In addition to its legal arguments, Facebook has submitted its user agreement and data policy, deposition excerpts and other extrinsic evidence to contend that BIPA's notice and consent requirements were actually satisfied. While that may or may not prove true in the end, the salient point for present purposes is that notice and consent are inextricably intertwined with the merits of plaintiffs' claims …. These dispositive disputes on the merits should be decided on summary judgment or at trial ….").

communication 'without the consent of all parties' or 'in any unauthorized manner. … We acknowledge 'the broad wording and purpose of the statute.'") (citation omitted); *Campbell v. Facebook Inc.*, 77 F. Supp. 3d 836, 848 (N.D. Cal. 2014) ("Moreover, the complaint's allegation that users' messages were intercepted in transit is to be taken as true at this stage of the case. Accordingly, the court DENIES Facebook's motion to dismiss plaintiffs' claim under section 631 of CIPA."). NaviStone further asserts that "[t]here simply is *no* law that prohibits Moosejaw from sending to its service provided the ordinary communications that it receives from website visitors." NaviStone MTD at 11-12. That must be rejected as it is nothing more than an attempt to conflate Section 631 with Section 632 in order to impose a confidentiality requirement when there is not one. *See, e.g.*, *People v. Guzman*, 11 Cal. App. 5th 184, 192 (Ct. App. 2017) ("Further, because wiretapping requires an unauthorized connection, the prohibition established by section 631 is not limited to 'confidential communications' as is the case for the prohibition against eavesdropping established by section 632.").

2. Plaintiff States A Claim Under Section 632

"Section 632 prohibits unauthorized electronic eavesdropping on confidential conversations." *In re Google Inc.*, 2013 WL 5423918, at *15 (N.D. Cal. Sept. 26, 2013) (citing Cal. Penal Code § 631(a)). "To state a claim under section 632, a plaintiff must allege an electronic recording of or eavesdropping on a confidential communication, and that not all parties consented to the eavesdropping." *In re Google Inc.*, 2013 WL 5423918, at *15 (N.D. Cal. Sept. 26, 2013) (citing *Flanagan v. Flanagan*, 41 P.3d 575, 577 (Cal. 2002)). "This language has uniformly been construed to prohibit one party to a confidential communication from recording that communication without knowledge or consent of the other party." *Membrila v. Receivables Performance Mgmt., LLC*, 2010 WL 1407274, at *2 (S.D. Cal. Apr. 6, 2010) (citing *Warden v. Kahn*, 99 Cal. App. 3d 805, 813 (Ct. App. 1979)).

Defendants assert that Plaintiff fails to state a claim under Section 632 because he "fails to allege sufficient facts demonstrating that any communication occurred at all or that an alleged communication was confidential." Moosejaw MTD at 6; NaviStone MTD at 12 ("Plaintiff's claim under section 632 fails because the clickstream data communicated to Moosejaw, and then by

Moosejaw to NaviStone, is neither the content of a communication nor confidential."). That is wrong on both fronts as Plaintiff has sufficiently alleged an objectively reasonable expectation of privacy in his communications with Moosejaw. *See, e.g.*, FAC ¶ 5 ("Throughout 2017, Mr. Revitch browsed Defendant Moosejaw's website at Moosejaw.com. During each of these visits, Mr. Revitch browsed Moosejaw.com because he intended to purchase outerwear. … Mr. Revitch was unaware at the time that his keystrokes, mouse clicks, and other electronic communications were being intercepted and disclosed to a third party. Mr. Revitch had a reasonable expectation of privacy when browsing Moosejaw.com and he intended his browsing to be confidential, in that he never expected that his keystrokes, mouse clicks, and other electronic communications were being intercepted and disclosed to a third party, or that Defendants would de-anonymize and identify him merely as a result of his browsing.") (emphasis added); FAC ¶ 46 ("Visitors have a reasonable expectation of privacy when browsing Moosejaw.com, in that they never expect that their keystrokes, mouse clicks, and other electronic communications were to be intercepted and disclosed to a third party, or that Defendants would de-anonymize and identify them as a result of their browsing.").

Nonetheless, Defendants argue that a website "user can have no baseline expectation of confidentiality in basic browsing information given the technological reality that such information is routinely redirected to third parties for a variety of purposes, from the display of content from third-party servers to banner advertising." NaviStone MTD at 13; *see also* Moosejaw MTD at 6 ("Plaintiff could not have had 'an objectively reasonable expectation that the conversation [was] not being recorded or overheard.'"). Unfortunately for Defendants, "California courts have rejected this argument." *Branca v. Ocwen Loan Servicing*, LLC, 2013 WL 12120261, at *13 (C.D. Cal. Dec. 27, 2013). "[U]nder section 632 'confidentiality' appears to require nothing more than the existence of a reasonable expectation by one of the parties that no one is 'listening in' or overhearing the conversation." *Coulter v. Bank of Am.*, 28 Cal. App. 4th 923, 929 (1994) (quoting *Frio v.Super. Ct.*, 203 Cal. App. 3d 1480, 1490 (1988)). "Thus, an actionable violation of section 632 occurs the moment the surreptitious recording or eavesdropping takes place, regardless whether it is later disclosed." *Kight v. CashCall, Inc.*, 200 Cal. App. 4th 1377, 1390 (2011)).

> Even if the speaker knows the information will be ultimately transmitted to other[s] …, section 632 "protects against intentional, nonconsensual" monitoring or recording of telephone conversations "regardless of the content of the conversation" or the fact that the information will be later disclosed …. The fact that plaintiffs may have known the information discussed in their phone calls would be disclosed to other[s] … does not mean the plaintiffs had no reasonable expectation that their telephone conversation were not being secretly overheard.

Branca, 2013 WL 12120261, at *13 (quoting *Kight v. CashCall, Inc.*, 200 Cal. App. 4th at 1392-93, 1397). Indeed, "the California Supreme Court adopted the interpretation of 'confidential communication' in which CIPA prohibits nonconsensual recording of conversations *regardless* of the content of the conversation or any expectation that the conversation may later be conveyed to a third party." *Bernstein v. United Collection Bureau, Inc.*, 2013 WL 5945056, at *4 (S.D. Cal. Nov. 5, 2013) (quoting *Flanagan*, 27 Cal. 4th at 776).

Defendants further complain that Plaintiff has not alleged what specific communications of his were intercepted. Moosejaw MTD at 6; NaviStone MTD at 13 (arguing Plaintiff's Section 632 claim "also perishes because … paragraphs 35 through 38 of the FAC, when properly understood, do not actually allege that NaviStone is sent the content of any communications between website visitors and Moosejaw.").[5] However, "Plaintiff need not plead the details of the conversation or allege that the conversation might be later relayed to third party." *Bernstein v. United Collection Bureau, Inc.*, 2013 WL 5945056, at *4 (S.D. Cal. Nov. 5, 2013) (emphasis added); *see also Mirkarimi v. Nevada Prop. 1 LLC*, 2013 WL 3761530, at *3 (S.D. Cal. July 15, 2013) ("As the *Flanagan* court stated, confidentiality under CIPA extends to a conversation regardless of whether information will be shared to a third party. … [S]o long as Plaintiff can demonstrate an objectively reasonable expectation that his conversation was not being overheard, he has a proper claim under CIPA."). Since Plaintiff has already demonstrated an objectively reasonable expectation of confidentiality, this argument fails. "Given that Plaintiff alleges disclosure of private information and that a determination regarding Plaintiff's reasonable expectation is arguably a question of fact,"

[5] NaviStone's argument separately fails for its reliance on the White Declaration for the reasons previously discussed. *See supra* Argument II.B.a, at n.4.

the Court should deny Defendants' request to dismiss his Section 632 claim. *Mirkarimi v. Nevada Prop. 1 LLC*, 2013 WL 3761530, at *3 (S.D. Cal. July 15, 2013).

Finally, "[t]he issue whether there exists a reasonable expectation that no one is secretly listening to a phone conversation is generally a question of fact." *Branca*, 2013 WL 12120261, at *12 (emphasis added). *See also Vera v. O'Keefe*, 2012 WL 3263930, at *4 (S.D. Cal. Aug. 9, 2012) (noting that a plaintiff's reasonable expectation of privacy is a question of fact for the jury to decide). As the *Opperman* court explained, this is a factual question not yet ripe for resolution:

> The "customs and habits [at issue] are very much in flux. The technology underlying the allegations in this case is still developing. … When applying community standards, it is possible that a jury of persons selected from that community might … find the intrusion highly offensive based on both the degree of intrusion (uploading the email addresses of a user's contacts to the Defendants' servers) and the setting in which the invasion took place (users' personal cellular phones). … A judge should be cautious before substituting his or her judgment for that of the community.
>
> In sum, this is not – or is not yet – a question that can be decided as a matter of law, and there is a triable issue of fact regarding whether Yelp's upload of the Plaintiffs' address book data was highly offensive to a reasonable person.

Opperman, 205 F. Supp. 3d at 1079-80; *see also In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 151 (3d Cir. 2015) ("Based on the pled facts, a reasonable factfinder could indeed deem Google's conduct 'highly offensive' or 'an egregious breach of social norms.'").

3. Plaintiff States A Claim Under Section 635

Moosejaw argues Plaintiff's Section 635 claim fails because "CIPA's private right of action cannot be extended to permit suits predicated on the mere 'possession' of an alleged eavesdropping device. … Plaintiff fails to explain why mere possession of the device, without more, led to any of his injuries." Moosejaw MTD at 7. That is meritless. Section 635 plainly provides that "[e]very person who … possesses … or furnishes to another any device which is primarily or exclusively designed or intended for eavesdropping … shall be punished by a fine not exceeding two thousand five hundred dollars ($2,500) …" Cal. Penal Code § 635 (emphasis added). *See also* FAC ¶ 78 ("NaviStone's code is a 'device' that is 'primarily or exclusively designed' for eavesdropping. That is, the NaviStone code is designed to gather PII, including keystrokes, mouse clicks, and other

electronic communications. The NaviStone code is also designed to scan visitors' computers in search of files that could be used to de-anonymize them.").

Moosejaw further argues that "CIPA only grants a private right of action to 'any person who has been injured by a violation of this chapter.'" Moosejaw MTD at 7 (quoting Cal. Penal Code § 637.2(a)). That defies a plain reading of Section 637.2. According to the California Court of Appeals, "[S]ection 637.2 … provides that it is not a necessary prerequisite to an action pursuant to this section that the plaintiff has suffered, or been threatened with actual damages." *Ion Equip. Corp. v. Nelson*, 110 Cal. App. 3d 868, 882 (Ct. App. 1980) (emphasis added); *see also* Cal. Penal Code § 637.2(b) (permitting any person to "bring an action to enjoin and restrain any violation of this chapter, and may in the same action seek damages as provided by subdivision (a)") (emphasis added). Here, Plaintiff is seeking both damages and injunctive relief. *See* FAC ¶¶ 82-83 ("Unless restrained and enjoined, Defendants will continue to commit such illegal acts. … Pursuant to Cal. Penal Code § 637.2, Plaintiff and Class Members have been injured by the violations of Cal. Penal Code § 635, and each seek damages for the greater of $5,000 or three times the amount of actual damages, as well as injunctive relief.").

According to Moosejaw, there is no Article III standing because "[h]ere, the challenged conduct (possession of a device) cannot be said to have caused an injury ('violation of the right to privacy' and 'loss of value in their PII')." Moosejaw MTD at 7 (quoting FAC ¶ 81); *see also id.* at 8 ("Allowing suit for mere possession of an eavesdropping device, without any allegation of injury, would obviate the need for Article III standing and raise severe constitutional concerns."). That is wrong. "The California District Courts that have interpreted CIPA in the wake of *Spokeo* have all held that CIPA violations constitute injuries in fact even without a showing of any actual harm beyond the invasion of the plaintiff's right to privacy." *CS Wang & Assoc. v. Wells Fargo Bank, N.A.*, 305 F. Supp. 3d 864, 881 (N.D. Ill. 2018).

Indeed, "the California Legislature specifically enacted CIPA to protect against the invasion of privacy. … Not only that, but CIPA provides for injunctive relief and statutory damages in addition to actual damages, suggesting that 'the California Legislature intended to grant persons in Plaintiff's position a right to judicial relief without additional allegations of injury.' … Thus,

violation of someone's right to privacy is not just a 'bare procedural violation,' … it is 'an affront to human dignity,' …. Accordingly, both historical practice and legislative judgment 'indicate that the alleged violations of [a p]laintiff's statutory rights under … CIPA constitute concrete injury in fact.'" *Raffin v. Medicredit, Inc.*, 2016 WL 7743504, at *3 (C.D. Cal. Dec. 19, 2016) (internal citations omitted).[6] As Judge Donato recently explained:

> The Supreme Court has expressly recognized that the violation of statutory procedural rights in itself can be sufficient, without any additional harm alleged. … Our circuit has also found that "privacy torts do not always require additional consequences to be actionable." … Intrusion on privacy alone can be a concrete injury.

Patel v. Facebook Inc., 290 F. Supp. 3d 948, 954 (N.D. Cal. 2018) (quotations omitted).

Defendants also contend that "Plaintiff fails to offer any facts that the Code provided to Moosejaw is 'primarily or exclusively designed' for eavesdropping." NaviStone MTD at 13; Moosejaw MTD at 8. According to Defendants, NaviStone's code "is simply part of the system of 'analytics tools, advertising networks, code libraries, and other utilities' that are 'part of routine internet functionality.'" NaviStone MTD at 13 (quoting *In re Facebook Internet Tracking Litig.*, 263 F. Supp. 3d 836, 846 (N.D. Cal. 2017)).[7] That is meritless. "NaviStone's code is a 'device' that is 'primarily or exclusively designed' for eavesdropping. That is, the NaviStone code is designed to gather PII, including keystrokes, mouse clicks, and other electronic communications. The NaviStone code is also designed to scan visitors' computers in search of files that could be used to de-anonymize them." FAC ¶ 78.

[6] Moosejaw's contention that "[b]y alleging that possession of a wiretapping device injured him, Plaintiff effectively collapses Sections 631, 632, and 635 together" fails. Moosejaw MTD at 7 n.4. Contrary to Moosejaw's interpretation of the statute, "possession and use of a wiretap device is [not] covered by Sections 631 and 632." Rather, "[a]s noted, section 632 prohibits 'eavesdropping,' … The practice is different from wiretapping, which is prohibited by section 631, insofar as it does not require an unauthorized connection to a transmission line, whereas wiretapping does. … Further, because wiretapping requires an unauthorized connection, the prohibition established by section 631 is not limited to 'confidential communications' as is the case for the prohibition against eavesdropping established by section 632." *People v. Guzman*, 11 Cal. App. 5th 184, 192, 217 Cal. Rptr. 3d 509, 515 (Ct. App. 2017). More importantly, unlike Sections 631 and 632, Section 635 addresses possession of a wiretapping device without regard to its use.

[7] The portion of *Facebook* quoted by Defendants concerned whether the plaintiffs "established that they ha[d] a reasonable expectation of privacy in the URLs of the pages they visit[ed]" – it was not in the context of a Section 635 claim. *In re Facebook Internet Tracking Litig.*, 263 F. Supp. 3d 836, 846 (N.D. Cal. 2017).

NaviStone further complains that typical websites "necessarily receive some record that a user communicated with a website and the nature of that communication." NaviStone MTD at 14. However, "Defendants' actions are not part of routine Internet functionality. Wiretaps are not necessary or needed to operate an e-commerce website. The NaviStone code is novel." FAC ¶ 45. Plaintiff elaborates that Defendants' actions "are not necessary practices for owners, operators, and developers of Internet websites, nor are they incidental to the act of facilitating a website or e-commerce transactions. None of these actions was undertaken in the ordinary course of business. On the contrary, these actions are contrary to the legitimate expectations of website visitors, and are contrary to established industry norms. So much so that they were the subject of multiple exposés in industry publications[.]" FAC ¶ 43 (emphasis added). These allegations support the plausible inference that NaviStone's code is anything but "part of routine internet functionality."

C. NaviStone's Additional Arguments For Dismissal Lack Merit

1. NaviStone's Standing Arguments Are Contrary To *Spokeo* and *Matera*

NaviStone's arguments regarding Article III standing fall under three categories, none of which support dismissal. First, NaviStone argues that Plaintiff did not suffer a cognizable injury because, in NaviStone's view, an "abstract violation of the right of privacy" is not enough to support a claim. NaviStone MTD at 5-6. The law on this issue is well-developed in this District. The fact that NaviStone cites hardly any of it is telling. Numerous courts have rejected the same or similar argument advanced by NaviStone here. For example, in *Matera v. Google, Inc.*, 2016 WL 5339806, at *8-14 (N.D. Cal. Sept. 23, 2016), the plaintiff brought claims under CIPA for allegedly intercepting, scanning, and analyzing private emails, and the defendant moved to dismiss based on the theory that plaintiff suffered no cognizable injury. The *Matera* framed its analysis around two controlling principles set forth in *Spokeo, Inc. v. Robbins*, 136 S. Ct. 1540 (2016). First, "an injury need not be 'tangible' in order to be 'concrete,' and intangible injuries may constitute an injury in fact." *Matera*, 2016 WL 5339806, at *8 (quoting *Spokeo*, 136 S. Ct. at 1549). "Second, the *Spokeo* Court reaffirmed that Congress may elevate injuries previously inadequate in law to legally cognizable 'concrete' injuries." *Id.* (internal quotations and brackets omitted).

Under *Spokeo*, "the violation of a right granted by statute may be sufficient to constitute [an] injury in fact," and "a plaintiff may plead injury in fact by alleging the violation of a statute without alleging 'any additional harm beyond the one Congress has identified.'" *Id.* (quoting *Spokeo*, 136 S. Ct. at 1549) (emphasis in original). Further, violations of CIPA are a form of invasion of privacy, which "has been recognized as a common law tort for over a century." *Id.* at *10; *see also Van Patten v. Vertical Fitness Grp., LLC*, 847 F.3d 1037, 1043 (9th Cir. 2017) ("Actions to remedy defendants' invasions of privacy [and] intrusion upon seclusion … have long been heard by American courts"). Other courts in this District have reached similar conclusions about Article III standing, *Spokeo* and claims under CIPA. *See*, *e.g.*, *In re Facebook Internet Tracking Litig.*, 263 F. Supp. 3d 836, 842 (N.D. Cal. 2017) (surveying authorities holding that "economic injury is not required to establish standing under" CIPA).[8]

Second, NaviStone argues that even if privacy claims are cognizable, Plaintiff fails to allege whether he provided personal information, the nature of that information, and whether the information was captured. NaviStone MTD at 5. That argument ignores the allegations and governing pleading standards. Rule 8 only requires a "short and plain statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. P. 8(a). As this Court has held, "[s]pecific facts are not necessary; the statement need only give the defendant fair notice of what the … claim is and the grounds upon which it rests." *Taylor v. Miller*, 2016 WL 1598746, at *1 (N.D. Cal. Apr. 21, 2016) (Chhabria, J.). On a motion to dismiss, courts "draw[] all reasonable inferences in favor of the plaintiffs." *Goldthorpe v. Cathay Pac. Airways Ltd.*, 2018 WL 5307018, at *1 (N.D. Cal. Jan. 16, 2018).

Here, NaviStone does not argue the allegations fail to give it fair notice of what the claim is and the grounds upon which it rests. Plaintiff alleges he visited Moosejaw.com "on several

[8] NaviStone also contends that the "legislative findings for CIPA, a 1967 statute, lack … detailed findings" showing that the statute was enacted to protect "concrete interests." MTD at 6. That is wrong. *See Matera*, 2016 WL 5339806 at *19 (discussing legislative history of CIPA); *see also Ribas v. Clark*, 38 Cal. 3d. 255, 365 (Cal. 1985) (The "manifest legislative purpose" of CIPA was "to accord every citizen's privacy the utmost sanctity" and "provide those who suffer an infringement of this aspect of their personal liberty a means of vindicating their right"). The only decision NaviStone cites for its argument had nothing to do with CIPA. *See Apple, Inc. v. Superior Ct.*, 56 Cal. 4th 128 (Cal. 2013) (addressing Song-Beverly Credit Card Act).

occasions prior to the filing of this lawsuit," and that "[d]uring each of Plaintiff's visits Defendants scanned his device for files that could be used to de-anonymize and identify him [and] captured his electronic communications …." FAC ¶ 1. Plaintiff also alleges that he browsed Moosejaw.com "because he intended to purchase outerwear," supporting a reasonable inference that his keystrokes and other interactions were typical of what you would expect from any consumer who shops online. *Id.* ¶ 5. Even if the allegations concerning the nature of Plaintiff's keystrokes are insufficient, NaviStone ignores the allegations that Defendants affirmatively "scanned Mr. Revitch's computer." The allegations also go far beyond the "short and plain" statement required by Rule 8 by explaining at length how the "back door" code works and what it is for. *Id.* ¶¶ 11-25. The FAC then follows with lengthy allegations describing how that code works in the context of the website that Plaintiff visited, Moosejaw.com. *Id.* ¶¶ 26-38. In short, NaviStone's arguments that the pleadings are insufficient to support standing lack merit.

Third, NaviStone makes several undeveloped, one-sentence arguments, which are easily dispatched. NaviStone notes that Plaintiff does not "claim to have received any direct mail promotion as a result of his browsing," but NaviStone does not (because it cannot) explain how that fact is relevant or supports dismissal. NaviStone MTD at 5. NaviStone then suggests there was no injury because the Plaintiff alleges NaviStone maintains a back-end database containing data and profiles on consumers across the U.S., which includes consumers' names and mailing addresses. NaviStone MTD at 5 (citing FAC ¶ 14). NaviStone's argument simply ignores the rest of the allegation, which explains how NaviStone uses to the database in conjunction with the NaviStone code to de-anonymize users and obtain personal information about them. *See* FAC ¶ 14. Moreover, NaviStone cites no authority for the proposition that a company is free to monitor communications and violate privacy rights if it has a list of potential names and addresses of the people whose rights are violated. Finally, NaviStone argues that a CIPA action "require[s] a substantial or highly offensive invasion of privacy," but again cites no supporting authority. NaviStone MTD at 7. No such limitation is found in the statute, and principles of statutory construction do not permit courts to insert such a limitation. *See Maita Distributors, Inc. of San Mateo v. DBI Bev., Inc.*, 667 F. Supp. 2d 1140, 1144 (N.D. Cal. 2009) (when interpreting statutes "[t]he court is to avoid reading into the

statute words that are not there"). Even if CIPA requires a "substantial or highly offensive invasion of privacy," NaviStone's arguments fail for the same reasons set forth in Section II.A above.

2. Moosejaw's Privacy Policy Does Not Foreclose Plaintiff's Claims

NaviStone (but not Moosejaw) contends that the "privacy policy" posted on Moosejaw's website serves to "foreclose[] Plaintiff's claims." NaviStone MTD at 8. That is wrong.

Initially, nowhere in NaviStone's briefing does it explain why a privacy policy would somehow preclude Plaintiff Revitch's causes of action. NaviStone instead merely just postulates that "Plaintiff's claims, if allowed, would upend th[e] balance" of CalOPPA, whereby "the [California] legislature" intended to enact "a disclosure regime [that] would provide meaningful protection that will help foster the continued growth of the internet economy." *Id.* at 9 (internal quotations omitted). However, NaviStone fails to provide any explanation why the existence of a privacy policy would preclude consumer claims under CalOPPA. *See id.* at 8-10. NaviStone's brief certainly does not quote any such language from the text of the CalOPPA statute. *See id.*

Nor does NaviStone cite any relevant case law in support of its argument. *See* NaviStone MTD at 8-10. The only citation in this section of NaviStone's briefing is to *Apple Inc. v. Superior Court*, 292 P.3d 883, 895 (2013), which says nothing of the sort. In *Apple*, the California Supreme Court held that a specific provision of the Song-Beverly Credit Card Act of 1971, section 1747.08, which "prohibits retailers from requesting or requiring [a] cardholder to provide personal identification information" at the time of sale, does *not* apply to "online purchases in which the product is downloaded electronically." *Id.* at 843. Significantly, nowhere in its discussion of CalOPPA did the California Supreme Court find that the presence of a privacy policy would preclude all privacy-oriented consumer suits and causes of action. *See id.* at 854-857. To argue otherwise would be a gross misreading of the opinion. *See id.* The *Apple* matter only concerns a specific portion of the Song-Beverly Credit Card Act, as it pertains to online purchases, which is not at issue in this matter.

Rather, this case is similar to *In re Google Inc. Gmail Litigation*, 2013 WL 5423918, at *1 (N.D. Cal. Sept. 26, 2013), in which the plaintiffs brought causes of action based on "federal and state anti-wiretapping laws" against Google for its alleged practice of "intercept[ing], read[ing], and

acquir[ing] content from emails that were in transit" in order to "provide targeted advertising." *Id.* In the court's order granting in part and denying in part defendant Google's motion to dismiss, it rejected Google's argument that its privacy policy served as "consent" to the alleged wiretapping:

> In its Motion to Dismiss, Google marshals both explicit and implied theories of consent. Google contends that by agreeing to Google's Terms of Service and Privacy Policies, Plaintiffs who are Gmail users expressly consented to the interception of their emails. Google further contends that because of the way that email operates, even non-Gmail users knew that their emails would be intercepted, and accordingly that non-Gmail users impliedly consented to the interception. Therefore, Google argues that in all communications, both parties – regardless of whether they are Gmail users – have consented to the reading of emails. The Court rejects Google's contentions with respect to both explicit and implied consent. Rather, the Court finds that it cannot conclude that any party – Gmail users or non-Gmail users – has consented to Google's reading of email for the purposes of creating user profiles or providing targeted advertising.

Id. at *13 (internal citations omitted; underlining added). Here, as well, a privacy policy cannot serve as "consent" for a surreptitious wiretap. *See* FAC ¶ 1 ("The wiretaps … are secretly embedded in the computer code of Moosejaw.com ….").

Furthermore, the disclosures in Moosejaw's privacy policy are inconsistent with the nature of Defendants' alleged wiretaps. Specifically, the privacy policy states that:

> You share Information with us in various ways. For example:
>
> - When you email us, ask a question or comment to Moosejaw or submit a customer review;
> - When you create an account or make a wish list, information such as name, email, postal address, telephone number, and gender;
> - When you make a purchase, billing and shipping addresses, including relevant e-mail, phone and credit card numbers and expiration dates;
> - When you enter any Moosejaw contests or other promotional features available on the Site.

Dkt. 25-2. However, the privacy policy does not disclose that Defendants have installed wiretaps that "enable [them] to immediately, automatically, and secretly observe the keystrokes, mouse clicks, and other electronic communications of visitors regardless of whether the visitor ultimately makes a purchase from Moosejaw." FAC ¶ 1.

Lastly, even if the privacy policy were to disclose the existence of Defendants' wiretaps (and it does not), such a disclosure is inadequate because "NaviStone's wiretaps engage as soon as the

visitor arrives at the main page of Moosejaw.com, website visitors are not provided with an opportunity to review any privacy policies or disclosures prior to deployment of the wiretaps." As such, "[b]y the time a user reaches the privacy policy, the wiretaps have already been deployed, and the de-anonymization has already occurred." *Id.* ¶ 23.[9]

3. Navistone's Statute Of Limitations Defense Cannot Be Resolved On The Pleadings

NaviStone asks the Court to dismiss Plaintiff's CIPA claim because Plaintiff fails to allege that his claims falls within CIPA's one-year statute of limitation period. No such allegation is required. "[T]he statute of limitations is an affirmative defense which the defendant has the burden of pleading and proving," and thus "a plaintiff need not affirmatively plead facts showing the absence of such a defense in order to state a claim." *Adobe Sys., Inc. v. Christenson*, 2011 WL 540278, at *2 (D. Nev. Feb. 7, 2011). In *F.D.I.C. v. Varrasso*, 2012 WL 219046 at *7 (E.D. Cal. Jan. 23, 2012), the defendant unsuccessfully made a similar argument when it contended that "[since] plaintiff did not include the date on which the FDIC became the receiver for IndyMac in the Complaint, … it was not evident from the face of the Complaint that the statute of limitations had not expired." The district court rejected that argument based on the rule that "'plaintiffs need not anticipate and attempt to plead around all potential defenses.'" *Id.* (quoting *Xechem, Inc. v. Bristol-Myers Squibb Co.*, 372 F.3d 899, 901 (7th Cir. 2004)). NaviStone is essentially making the same argument here.

Although a statute of limitations defense *might* support a motion to dismiss where the defense "is apparent on the face of the complaint," dismissal is not proper if the "allegations are susceptible of an interpretation that would make [the plaintiff's] claim timely." *Shaw v. Specialized Loan Servicing, LLC*, 2014 WL 12586435, at *7 (C.D. Cal. Sept. 12, 2014). Here, NaviStone does not argue that it is clear from the face of the complaint that Plaintiff's claims are untimely, but

[9] In a footnote, NaviStone argues that "this allegation at most covers [Plaintiff's] *first visit* to the *first page* of the website." NaviStone MTD at 10 n.10 (italics in original). As such, NaviStone argues, "Plaintiff's own theory requires him to allege with specificity the date of his first visit to Moosejaw.com." *Id.* However, such requirements are a proper topic for discovery and go far beyond the applicable pleading standards. *See* Fed. R. Civ. P. 8(a) ("A pleading that states a claim for relief must contain … a short and plain statement of the claim showing that the pleader is entitled to relief.").

instead appears to acknowledge that the allegations are susceptible to an interpretation that the claims are timely. *See* NaviStone MTD at 7-8. Plaintiff filed his complaint on November 9, 2018. *See* Original Complaint (Doc. No. 1). He alleges that he browsed Moosejaw.com "[t]hroughout 2017," and that he did not learn about the conduct at issue here until December 2017. FAC ¶ 5. As to these allegations, NaviStone argues in a footnote that the "FAC is silent on how he learned" about the issue, and that the allegation is "implausible." MTD at 8. However, under the authorities cited above, Plaintiff is not required to allege how he learned about the issue, and NaviStone's disagreement about the "plausibility" of the allegation simply raises a factual dispute not susceptible to resolution on the pleadings. *Tippitt v. Life Ins. Co. of N. Am.*, 2017 WL 3189464, at *1 (N.D. Cal. May 30, 2017) (Chhabria, J.) ("A motion to dismiss is not an appropriate mechanism for resolving factual disputes ….").

III. CONCLUSION

For the foregoing reasons, Defendants' motions to dismiss should be denied in their entirety. Alternatively, if the Court determines that the pleadings are deficient in any respect, Plaintiff respectfully requests leave to amend to cure any such deficiencies. *See Roney v. Miller*, 705 F. App'x 670, 671 (9th Cir. 2017) (holding lower court erred in denying leave to amend after dismissing first amended complaint).

Dated: March 27, 2019

Respectfully submitted,

BURSOR & FISHER, P.A.

By: /s/ *Joel D. Smith*
Joel D. Smith

L. Timothy Fisher (State Bar No. 191626)
Joel D. Smith (State Bar No. 244902)
Frederick J. Klorczyk III (State Bar. No. 320783)
Neal J. Deckant (State Bar No. 322946)
1990 North California Boulevard, Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-Mail: ltfisher@bursor.com
jsmith@bursor.com
fklorczyk@bursor.com
ndeckant@bursor.com

BURSOR & FISHER, P.A.
Scott A. Bursor (State Bar No. 276006)
888 Seventh Avenue
New York, NY 10019
Telephone: (212) 989-9113
Facsimile: (212) 989-9163
E-Mail: scott@bursor.com

Attorneys for Plaintiff